Adobe Deliverability Best Practice Guide

2020 Edition

Table of Contents

1. Introduction

Email deliverability, a critical component to every sender's marketing program success, is characterized by ever-changing criteria and rules. ISPs have a continual need to prevent spammers, so they're obliged to develop sophisticated filtering techniques to protect their customers. Email senders can become unintentionally ensnared in those efforts. Effectively navigating in this digital world requires regular tuning of your email strategy, with consideration to key deliverability trends, to best reach your audiences.

According to Lifewire, more than 3.8 billion email addresses exist today. On top of that, social media consultants Lori Lewis and Chad Callahan report that 188 million emails are sent every minute, which encompasses more than half of the world's population. But gone are the days of sending maximum amounts of email for minimal conversion. Reality is that consideration of volume alone puts your highly engaged customers at risk of not receiving their emails. This can have major revenue implications for you as a sender. Viewing email as a low-cost channel with unlimited potential is challenging and fragile.

In this digital era, people expect to be wowed—quickly. They want that "ah ha" moment with everyone they choose to interact with, and competition is fierce. Between devices like computers, cell phones and smart home equipment, and the content supported, such as instant messaging, email, web, push and social media applications, consumers are incessantly bombarded with content. If a message isn't compelling, they're apt to delete it or entirely disengage.

Let's face it. Today, more than ever, you need to stand out. This means giving your customers unique, personalized, and extremely relevant customer experiences. Otherwise, you risk losing a customer forever. It's imperative to have an integrated, dynamic multichannel strategy that motivates your audience to stay engaged.

Use this guide to learn key deliverability terms, concepts, and approaches to empower you to stay ahead of the curve. Use it to keep the email channel at the forefront of your marketing mix, with high priority on deliverability, inbox placement, and your revenue.

2. Deliverability strategy

Designing successful email marketing campaigns depends on having a clear understanding of marketing goals, whether they're for prospecting or customer relationship management (CRM) initiatives. This helps to determine *who* to target, *what* to promote, and *when* outreach is ideal. Here are some examples of email marketing strategy objectives:

- Acquiring new customers
- Converting prospects to first time buyers
- Growing current customer relationships with additional client offerings
- Retaining loyal customers
- Enhancing customer satisfaction and brand loyalty
- Reactivating lost or lapsed customers

3. Deliverability defined

There are two key metrics that play a role in the definition of *deliverability*. The *delivered rate* is the percentage of emails that don't bounce and are accepted by the ISP. Next is *inbox placement*—this is applied to the messages that are accepted by the ISP and determines whether the email lands in the inbox or the spam folder.

It's important to understand both delivered rate and the inbox placement rate in conjunction with one another when measuring email performance. A high delivered rate is not the only facet of deliverability. Just because a message is received via an ISP's initial checkpoint doesn't necessarily mean that your subscriber actually saw and interacted with your communication.

4. Why deliverability matters

If you don't know whether your emails are getting delivered or whether they are landing in the inbox versus the spam folder, you should. Here's why.

Countless hours go into the planning and production of your email campaigns. If the emails bounce or ultimately land in your subscribers' spam folder, your customers probably won't read them, your call to action (CTA) won't be acknowledged, and you'll fall short of your revenue goals due to lost conversions. Put simply, you can't *afford* to ignore deliverability. It's crucial to the success of your email marketing efforts—and your bottom line.

Following deliverability best practices ensures that your email will have the best possible chance of opens, clicks, and the ultimate goal—conversion. You can write a brilliant subject line and have beautiful imagery and engaging content. But if that email doesn't get delivered, the customer doesn't have any opportunity to convert. All in all, in email deliverability, each step in the mail acceptance process is dependent on the former for program success.

4.1. Step 1: Email delivered

Important factors for delivery:

- Solid infrastructure: IP and domain configuration, feedback loop (FBL) setup (including complaint monitoring and processing), and regular bounce processing. For Adobe clients, Adobe is responsible for this setup on behalf of our clients.
- Strong authentication: Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), Domain-based Message Authentication, Reporting, and Conformance (DMARC).
- High list quality: Explicit opt-in, valid email acquisition methods, and engagement policies.
- Consistent sending cadence and minimization of volume fluctuations.
- High IP and domain reputation.

4.2. Step 2: Email inbox placement

ISPs have unique, complex, and ever-changing algorithms to determine whether your email is placed in the inbox or the junk or spam folder.

Here are some important factors for inbox placement:

- Delivered email
- High engagement
- Low complaints (less than 0.1 percent overall)
- Consistent volume
- Low spam traps
- Low hard bounce rate
- Lack of blocklist issues

4.3. Step 3: Email engagement—opens

Here are some important factors for open rate:

- Email delivered and landed in the inbox
- Brand recognition
- Compelling subject line and preheaders
- Personalization
- Frequency
- Relevance or value of content

4.4. Step 4: Email engagement—clicks

Here are some important factors for click rate:

- Email delivered, landed in the inbox, and opened
- Strong CTA
  - This is the primary action you want to achieve from your audience. Normally, it's a click on a URL. Make sure it's clear and easy for the user to find.
- Relevance or value of content

4.5. Step 5: Conversion

Here are some important factors for conversion:

- All the above
- Transition from email via a working URL to a landing page or sales page
- Landing page experience
- Brand recognition, perception, and loyalty

4.6. Potential impact on revenue

Conversion is key, but what's the alternative? Your deliverability strategy can strengthen or wreak havoc on email marketing program nirvana. The following chart illustrates the potential loss in revenue that a weak deliverability policy can have on your marketing program. As demonstrated, for a business with a 2 percent conversion rate and average purchase of $100, every 10 percent reduction in inbox placement equals an almost $20,000 loss in revenue. Keep in mind that these numbers are unique for every sender.

Sent	Percent delivered	Delivered	Percent inbox	Inbox	Number not in inbox	Conversion rate	Number of lost Conversions	Average purchase	Lost revenue
100K	99%	99K	100%	99K	-	2%	0	$100	$ -
100K	99%	99K	90%	89.1K	9,900	2%	198	$100	$ 19,800
100K	99%	99K	80%	79.2K	19,800	2%	396	$100	$ 39,600
100K	99%	99K	70%	69.3K	29,700	2%	594	$100	$ 59,400
100K	99%	99K	60%	59.4K	39,600	2%	792	$100	$ 79,200
100K	99%	99K	50%	49.5K	49,500	2%	990	$100	$ 99,000
100K	99%	99K	40%	39.6K	59,400	2%	1188	$100	$118,800
100K	99%	99K	30%	29.7K	69,300	2%	1386	$100	$138,600
100K	99%	99K	20%	19.8K	79,200	2%	1584	$100	$158,400

5. Other metrics that matter for deliverability

One of the best ways to identify a sending reputation issue is through the metrics. Let's take a look at some key deliverability metrics to monitor and how to use them to identify a reputation issue.

5.1. Bounces

Bounces are the result of a delivery attempt and failure where the ISP provides back failure notices. Bounce handling processing is a critical part of list hygiene. After a given email has bounced several times in a row, this process flags it for suppression. The number and type of bounces required to trigger suppression vary from system to system. This process prevents systems from continuing to send invalid email addresses. Bounces are one of the key pieces of data that ISPs use to determine IP reputation. Keeping an eye on this metric is very important. "Delivered" versus "bounced" is probably the most common way of measuring the delivery of marketing messages: the higher the delivered percentage is, the better.

We'll dig into two different kinds of bounces.

5.2. Hard bounces

Hard bounces are permanent failures generated after an ISP determines a mailing attempt to a subscriber address as not deliverable. Hard bounces that are categorized as undeliverable are added to the quarantine, which means they wouldn't be reattempted. There are some cases

where a hard bounce would be ignored if the cause of the failure is unknown. Here are some common examples of hard bounces:

- Address doesn't exist
- Account disabled
- Bad syntax
- Bad domain

5.3. Soft bounces

Soft bounces are temporary failures that ISPs generate when they have difficulty delivering mail. Soft failures will retry multiple times (with variance depending on use of custom or out-of-box delivery settings) in order to attempt a successful delivery. Addresses that continually soft bounce will not be added to quarantine until the maximum number of retries has been attempted (which again vary depending on settings). Some common causes of soft bounces include the following:

- Mailbox full
- Receiving email server down
- Sender reputation issues

Bounce type	Hard bounce A "hard" error indicates an invalid address. This involves an error message that explicitly states that the address is invalid.	Soft bounce This might be a temporary error or one that could not be categorized.	Ignored This is an error that is known to be temporary.
Error type	• User unknown • Unreachable (5.5.x) • Account disabled • Refused (spam complaint)	• Invalid domain • Unreachable (4.4.x) • Mailbox full • Account disabled • Refused	• Out of office • Technical error

Bounces are a key indicator of a reputation issue because they can highlight a bad data source (hard bounce) or a reputation issue with an ISP (soft bounce).

Soft bounces often occur as part of sending email and should be allowed to resolve during the retry processing before characterizing as a true deliverability issue. If your soft bounce rate is greater than 30 percent for a single ISP and do not resolve within 24 hours, it's a good idea to raise a concern with your Adobe deliverability consultant.

5.4. Complaints

Complaints are registered when a user indicates that an email is unwanted or unexpected. This subscriber action is typically logged through either the subscriber's email client when they hit the spam button or via a third-party spam reporting system.

5.4.1. ISP complaint

Most Tier 1 and some Tier 2 ISPs provide a spam reporting method to their users as opt-out and unsubscribe processes have been used maliciously in the past to validate an email address. The Adobe platform will receive these complaints via ISP FBLs. This is established during the setup process for any ISPs that provide FBLs and allows the Adobe platform to automatically add email addresses that complained to the quarantine table for suppression. Spikes in ISP complaints can be an indicator of poor list quality, less-than-optimal list collection methods, or weak engagement policies. They're also often noted when content is not relevant.

5.4.2. Third-party complaints

There are several anti-spam groups that allow for spam reporting at a broader level. Complaint metrics used by these third parties are used to tag email content to identify spam email. This process is also known as fingerprinting. Users of these third-party complaint methods are generally savvier about email, so they can have a greater impact than other complaints may have if left unanswered.

ISPs collect complains and use them to determine the overall reputation of a sender. All complaints should be suppressed and no longer contacted as quickly as possible and in accordance with local laws and regulations.

5.5. Spam traps

Spam traps exist to help identify mail from fraudulent senders or those that aren't following email best practices. The spam trap email address is generally not publicly published and are almost impossible to identify. Delivering email to spam traps can impact your reputation with varying degrees of severity depending on the type of trap and the ISP. Learn more about the different types of spam traps in the following sections.

5.5.1. Recycled

Recycled spam traps are addresses that were once valid but are no longer being used. One key way to keep lists as clean as possible is to regularly send email to your entire list and appropriately suppress bounced emails. This helps abandoned email addresses to be quarantined and withheld from further use.

In some cases, an address can become recycled within 30 days. Sending regularly is a vital aspect of good list hygiene, along with regularly suppressing inactive users. Reengagement campaigns are typically a part of sophisticated email marketing programs. This campaign style allows the sender to attempt to win back users that would otherwise no longer be mailed.

5.5.2. Typo

A typo spam trap is an address that contains a misspelling or malformation. This often occurs with known misspellings of major domains like Gmail (ex: *gmial* is a common typo). ISPs and other blocklist operators will register known bad domains to be used as a spam trap in order to identify

spammers and measure sender health. The best way to prevent typo spam traps is to use a double opt-in process for list collection.

5.5.3. Pristine

A pristine spam trap is an address that has no end user and has never had an end user. It's an address that was created purely to identify spam email. This is the most impactful type of spam trap as it's virtually impossible to identify and would require a substantial effort to clean from your list. Most blocklists utilize pristine spam traps to list unreputable senders. The only way to avoid pristine spam traps from infecting your broader marketing email list is to utilize a double opt-in process for list collection.

A spam trap is an address used to identify an unpermissioned or unsolicited email.

5.6. Bulking

Bulking is the delivery of mail into the spam or junk folder of an ISP. It's identifiable when a lower-than-normal open rate (and sometimes click rate) is paired with a high delivered rate. The causes for why emails are bulked varies by ISP. In general, though, if messages are being placed in the bulk folder, a flag that influences sending reputation (list hygiene, for example) requires reevaluation. It's a signal that reputation is diminishing, which is a problem that needs to be corrected immediately before it affects further campaigns. Work with your Adobe deliverability consultant to remedy any bulking issues depending on your situation.

5.7. Blocking

A block occurs when spam indicators reach proprietary ISP thresholds and the ISP begins to block mail (noticeable through bounced mailing attempts) from a sender. There are various types of blocks. Generally, blocks occur specific to an IP address, but they can also occur at the sending domain or entity level. Resolving a block requires specific expertise, so please contact your Adobe deliverability consultant for assistance.

5.8. Blocklisting

A blocklisting occurs when a third-party blocklist manager registers spammer-like behavior associated with a sender. The cause of a blocklist is sometimes published by the blocklisting party. A listing is generally based on IP address, but in more severe cases it can be by IP range or even a sending domain. Resolving a blocklisting should involve support from your Adobe deliverability consultant in order to fully resolve and prevent further listings. Some listings are extremely severe and can cause long-lasting reputation issues that are difficult to resolve. The result of a blocklisting varies by the blocklist but has the potential to impact delivery of all email.

6. Engagement

6.1. Engagement is essential

Engagement has become the single most important factor impacting inbox placement decisions. Over the years, ISPs have shifted their focus from content-related filters to a behavioral model, heavily relying on positive and negative engagement actions. Positive engagement primarily includes opens, clicks, forwards, and replies. Negative engagement includes deleting without opening, ignoring, unsubscribing, and marking as spam. Receiving explicit permission is the foundation of positive email engagement. Once a brand has permission, that relationship should be nurtured by regularly measuring and meeting the customers' expectations through frequency and content.

A good open and click rate varies depending on many factors for different senders. Consult with your deliverability consultant to establish specific goals and baselines for your email program.

Email engagement is also a term used to describe one type of metric that helps to determine IP reputations. ISPs that own their own portals (Hotmail, AOL, Yahoo, Gmail, etc.) have a tremendous amount of data available regarding their customers' interactions with their mail. They can see opens, clicks, and many other forms of interaction, even if mail is moved in or out of the spam folder. They can also see if the email address it was sent to is in the clients address book or not.

While you as a sender cannot track all of the same engagement metrics, opens and clicks make a good starting point. It's important to note that ISPs only have visibility to *email* engagement. While other forms of engagement are important to as business as a whole, ISPs only have visibility and make filtering verdicts based on email metrics.

6.2. Quality over quantity

Organic list growth is the cornerstone of a healthy list. Many marketers put a tremendous focus on list growth, but from a deliverability perspective it's important to build a quality list of highly engaged subscribers. Continually sending emails to a largely unengaged audience can decrease your sending reputation and greatly increase the likelihood that your email will land in the spam or junk folder.

Mailing frequency is important to consider when creating and maintaining an email marketing program. Setting the recipients' expectations during your welcome message is a very useful strategy—people like to know what to expect. Yet those expectations need to be met: sending email too often can cause customer fatigue and in some instances may lead to increased complaints and unsubscribes.

The right frequency is something each marketer must find for their specific marketing program. We suggest testing different frequencies to find the right balance for any specific marketing program. Keeping recipients engaged and active is one of the most important things a marketer can do to ensure the success of an email marketing program.

6.3. Changing interests

Subscriber interests are constantly evolving, and marketers need to understand that commitment to a brand may be temporary. Some subscribers will opt out, but many will just delete or ignore

unwanted emails. From a consumer's perspective, any message that is unsolicited or unwanted is perceived as spam. Therefore, marketers need to rely on permission-based marketing and monitor engagement for loss of interest. In order to achieve optimal inbox placement, we recommend that marketers strategically reengage subscribers using reactivation campaigns and a "win-back strategy," which can be very useful tools to an email Marketer.

A win-back strategy is when a special incentive is regularly sent to a specific portion of a marketing database in an attempt to reengage a list where has been low open and click activity. Positive responses are kept, and the portion of the list that doesn't respond is moved to an inactive status and would no longer be mailed to.

A reactivation campaign is similar but is used to reconfirm a list one time, which is useful when dealing with old, stale lists—ones that haven't been mailed to for over 12 months, or even years. This type of campaign is also typically enforced by blocklists in order to resolve a block. The subscribers that are not successfully reengaged through this process should be excluded from future email promotions.

The best way to implement a win-back or reactivation campaign will be unique to your email program and should be fully customized for your business needs and situation.

6.4. Reply-to is engagement too

It's easy to just set your reply-to email to be a "no-reply" address, but this would be a mistake that overlooks the bigger picture.

When recipients reply to marketing emails, a response is expected. By enabling a reply-and-respond system, you will help boost your sender reputation. This will increase the likelihood of positive deliverability and inbox placement rates.

It's also just a much better customer experience and will help to increase positive consumer perception of your brand. After all, nothing says "please do business with us" like "we want to hear from you."

A final key part of the reply-to strategy is that if you do have a real email address they can reply to, make sure someone is monitoring it and it's not just an auto-response. If not monitored, the missed expectations can frustrate the customer and lead to complaints or lower engagement.

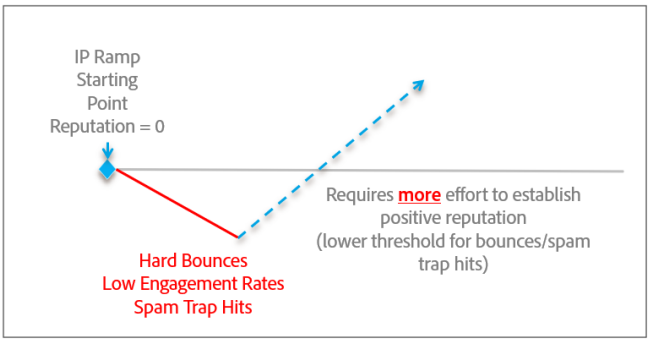
7. Transition process: switching email platforms

When moving email service providers (ESPs), it's not possible to also transition your existing, established IP addresses. It's important that you follow best practices for developing a positive reputation when starting afresh. Because the new IP addresses you will be using do not yet have reputation, ISPs are unable to fully trust the mail coming from them and need to be cautious in what they allow to be delivered to their customers.

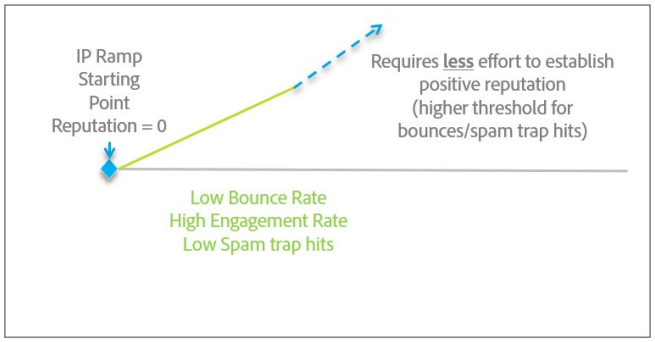
Think about what you do when meeting someone new. Typically, you need to build trust instead of trusting them right away. Don't think that your brand is going to automatically help with that trust, because spammers will user your name to do bad things. ISPs need to revaluate your sending practices, since action is most telling in email deliverability.

Establishing a positive reputation is a process. But once it's established, small negative indicators will have less impact to you and your mail delivery.

Here's what happens when you start off on the wrong foot.



While this is what you want to achieve.



The amount of time to warm your IP addresses and domains may vary, but up to an eight-week benchmark is common for typical senders to establish a reputation at most Tier 1 ISPs (Gmail, Microsoft, Verizon/Yahoo/AOL, etc.).

In the next sections, we'll investigate some key areas to focus on to onboard properly.

7.1. Infrastructure

Successful deliverability depends on a strong foundation. Email infrastructure is a core element. A properly constructed email infrastructure includes multiple components—namely domain(s) and IP address(es). These components are like the machinery behind the emails you send, and they're oftentimes the anchor of sending reputation. Deliverability consultants ensure that these elements are set up properly during implementation, but due to the reputation element, it's important for you to have this basic understanding.

7.1.1. Domain setup and strategy

Times have changed, and some ISPs (like Gmail and Yahoo) now incorporate domain reputation as an additional point when it comes to attaching email reputation to a sender. Your domain reputation is based on your sending domain instead of your IP address. This means that your brand takes precedence when it comes to ISP filtering decisions.

Part of the onboarding process for new senders on Adobe platforms include setting up your sending domains and ensuring that your infrastructure is established properly (see our "infrastructure"

section for additional details). You should work with an expert on what domains you plan to use in the long term. Here are some tips that shape a good domain strategy:

- Be as clear and reflective of the brand as possible with the domain you choose so that users don't incorrectly identify the mail as spam. Some examples are newsletter.foo.com, receipts.foo.com, and so on.
- You shouldn't use your parent or corporate domain as it could impact the delivery of mail from your organization to ISPs.
- Consider using a subdomain of your parent domain to legitimize your sending domain.
- Separate your subdomains for Transactional and Marketing message categories. This will help your email traffic flow on a more reliable basis as ISPs look for this sending method, which is a known email best practice and is highly recommended.

7.1.2. IP strategy

It's important to form a well-structured IP strategy to help establish a positive reputation. The number of IPs and setup varies depending on your business model and marketing goals. Work with an expert to develop a clear strategy to start off right. Consider these things that are important to note:

- Too many IPs can trigger reputation issues as it is a common tactic of spammers to *snowshoe*, which is a tactic used by spammers where traffic is spread across many IPs to maximize the delivery of spam mail. Even though you're not a spammer, you might look like one if you use too many IPs, especially if those IPs haven't had any prior traffic.
- Too few IPs can cause throughput issues and potentially trigger reputation issues. Throughput varies by ISP. How much and how quickly an ISP is willing to accept is typically based on their infrastructure and sending reputation thresholds.
- Separating traffic for messaging types is key. It's important to, at a bare minimum, separate marketing and transactional mail on separate IP pools.
- Depending on your mail strategy, it may also be advisable to separate different products or marketing streams on different IP pools if your reputation is drastically different. Some marketers also segment by region. Separating the IP for traffic with a lower reputation will not fix the reputation issue, but it will prevent issues with your "good" reputation email deliveries. After all, you don't want to sacrifice your good audience for a riskier one.

7.1.3. Feedback loops

Behind the scenes, Adobe platforms are processing data regarding bounces, complaints, unsubscribes, and more. The setup of these feedback loops is an important aspect to deliverability. Complaints can damage a reputation, so you should email addresses that register complaints from your target audience. It's important to note that Gmail doesn't provide this data back. List unsubscribe headers and engagement filtering are especially important for Gmail subscribers, who now comprise the majority of subscriber databases.

7.1.4. Authentication

Authentication is the process that ISPs use to validate the identity of a sender. The two most common authentication protocols are Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM). These are not visible to the end user but do help ISPs filter email from verified senders. Domain-based Message Authentication Reporting and Conformance (DMARC) is gaining popularity, although its policies aren't yet incorporated by all ISPs in their reputation systems.

SPF

Sender Policy Framework (SPF) is an authentication method that allows the owner of a domain to specify which mail servers they use to send mail from that domain.

DKIM

Domain Keys Identified Mail (DKIM) is an authentication method that is used to detect forged sender addresses (commonly called *spoofing*). If DKIM is enabled, it allows the receiver to confirm if the sender is authorized to send mail from that domain.

DMARC

Domain-based Message Authentication, Reporting and Conformance (DMARC) is an authentication method that allows domain owners the ability to protect their domain from unauthorized use. DMARC uses SPF or DKIM or both to allow a domain owner to control what happens to mail that fails authentication: delivered, quarantined, or rejected.

7.2. Targeting criteria

When sending new traffic, only target your highest engaged users during the early phases of IP warming. This helps establish a positive reputation from the get-go to effectively build trust before rolling in your less engaged audiences. Here's a basic formula for engagement:

$$\text{Engagement Rate} = \frac{\text{Opened or Clicked}}{\text{Delivered}}$$

Typically, an engagement rate is based on a specific period of time. This metric can vary drastically depending on if the formula is applied on an overall level or for specific mailing types or campaigns. The specific targeting criteria needs to be provided by working with your Adobe deliverability consultant, since every sender and ISP varies and usually requires a customized plan.

7.3. ISP-specific considerations during IP warming

ISPs have different rules and different ways of looking at their traffic. For example, Gmail is one of the most sophisticated ISPs because they look at engagement very strictly (opens and clicks) in addition to all other reputation measures. This requires a customized plan that only targets the highest engaged users at the onset. Other ISPs may require the same as well. Work with your Adobe deliverability consultant for a specific plan.

7.4. Volume

The volume of mail you're sending is critical to establishing a positive reputation. Put yourself in an ISPs shoes—if you start seeing a ton of traffic from someone you don't know, it would be alarming. Sending large volume of mail right away is risky and is sure to cause reputation issues that are often difficult to resolve. It can be frustrating, time consuming, and costly to dig yourself out of poor reputation and bulking and blocking issues resulting from sending too much too soon.

The volume thresholds vary by ISP and can also vary depending on your average engagement metrics. Some senders require a very low and slow ramp of volume, whereas others may allow for a steeper ramp in volume. We recommend working with an expert, like an Adobe deliverability consultant, to develop a customized volume plan.

Here's a list of hints and tips for how to transition smoothly:

- Permission is the foundation of any successful email program.
- Low and slow—start with low sending volumes and then increase as you establish your sender reputation.
- A tandem mailing strategy allows you to ramp up volume on Campaign while winding down with your current ESP, without disrupting your email calendar.
- Engagement matters—start with the subscribers who open and click your emails regularly.
- Follow the plan—our recommendations have helped hundreds of Campaign clients successfully ramp up their email programs.
- Monitor your reply email account. It's a bad experience for your customer to use noreply@xyz.com or to not respond.
- Inactive addresses can have a negative deliverability impact. Reactivate and repermission on your current platform, not your new IPs.
- Domains—use a sending domain that's a subdomain of your company's actual domain
    - For example, if your company domain is xyz.com, email.xyz.com provides more credibility to the ISPs than xyzemail.com
- Transparency—registration details for your email domain should be available publicly and shouldn't be private.

In many circumstances, transactional mail doesn't follow the traditional promotional warming approach. It's obviously difficult to control volume in transactional mail due to its nature, since it generally requires a user interaction to trigger the email touch. In some cases, transactional mail can simply be transitioned without a formal plan. In other cases, it might be better to transition each message type over time to slowly grow the volume. For example, you may want to transition as follows:

1. Purchase confirmations—high engagement generally
2. Cart abandon—medium-high engagement generally
3. Welcome emails—high engagement but can contain bad addresses depending on your list collection methods
4. Winback emails—lower engagement generally

8. First impressions—list collection and welcome emails

When looking to build a new relationship, making a good first impression is crucial. Without it, nothing else you say or do may be given a chance. The relationship between a brand and those choosing to interact with them is no different. Everything starts somewhere. And when it comes to running an email program, it starts with collecting email addresses and welcoming those subscribers to your program. Let's check out how you can set yourself up for running a successful email program by making a good first impression in those areas.

8.1. Address collection and list growth

The best sources of new email addresses are direct sources like sign-ups on your website or in physical stores. In those situations, you can control the experience to make sure it's positive and that the subscriber is actually interested in getting email from your brand.

Some notes about these sign-up methods:

Physical store list collection can present challenges due to verbal or written address inputs causing misspelling in the addresses. Sending a confirmation email as quickly as possible after in-store sign-ups is recommended.

The most common form of website sign-up is "single opt-in." This should be the absolute minimum standard you use to acquire email addresses. It's when the holder of a specific email address grants a sender permission to send them marketing emails, usually by submitting the address via a web form or in-store signups. While it's possible to run a successful email campaign using this method, it can be the cause of some problems.

- Unconfirmed email addresses can have typos or be malformed, incorrect, or maliciously used. Typos and malformed addresses cause high bounce rates, which can and do provoke blocks issued by ISPs or IP reputation loss.
- Malicious submission of known spam traps (sometimes called "list poisoning") can cause huge problems with delivery and reputation if the owner of that trap takes action. It's impossible to know if the recipient truly wants to be added to a marketing list without a confirmation. This makes it equally impossible to set the recipient's expectations and can lead to increased spam complaints—and sometimes blocklisting if the collected email happens to be a spamtrap.

For guidance on how to minimize the issues presented in both physical store and single opt-in, go to section 8.1.2 in this guide for the details and benefits of double opt-in.

Subscribers often use throw-away addresses, expired addresses, or addresses that aren't theirs in order to get what they want from a website but also avoid getting added to marketing lists. When this happens, marketers' lists can result in having a high number of hard bounces, high spam complaint rates, and subscribers who don't click, open, or positively engage with emails. This can be seen as a red flag for mailbox providers and ISPs.

8.1.1. Sign-up forms

In addition to all of the fields for the data you want to collect about your new subscribers, which can encourage more relevant connections with your customers, there are a few other things you should do with your sign-up form on the website.

- Set clear expectations with the subscriber that they're agreeing to receive email, what they will receive, and how often they will receive it.

- Add options allowing the subscriber to select the frequency or type of communications that they receive. This allows you to know the subscriber's preferences from the start so you can provide the best possible experience for your new customer.
- Balance the risk of losing the subscriber's interest during the sign-up process by asking for as much information as possible. Things like their birthday, location, interests, and so on, which might help you send more customized content. Every brand's subscribers will have different expectations and tolerance thresholds, so testing is key to find the right balance for your situation.

Don't use prechecked boxes during the sign-up process. While this can get you in trouble legally in some cases, it's also just a negative customer experience.

8.1.2. Data quality and hygiene

Collecting data is only part of the challenge. You also need to make sure the data is both accurate and usable. You should have basic format filters in place. An email address isn't valid if it doesn't include an "@" or "." for example. Be sure to not allow common alias addresses, which are also referred to as *role accounts* (like "info," "admin," "sales," "support," and so on). Role accounts can present risk because, by their nature, the recipient contains a group of people as opposed to a single subscriber. Expectations and tolerance can vary within a group, which risks complaints, varying engagement, unsubscribes, and general confusion.

Here are a few solutions to common issues you may run into with your email address data:

Double opt-in (DOI)

Double opt-in (DOI) is considered the best deliverability practice by most email experts. If you're having trouble with spam traps or complaints on your welcome emails, DOI is a good way to ensure that the subscriber receiving your emails is the person who actually signed up for your email program and wants to receive your emails.

DOI consists of sending a confirmation email to the subscriber's email address who has just signed up to your email program which contains a link that must be clicked to confirm consent. With this acquisition method, if the subscriber doesn't confirm, the sender wouldn't send them additional emails. Let new subscribers know you're doing this on the website, encouraging them to complete the sign-up before continuing. This method does see a reduction in the number of sign-ups, but those who do sign-up tend to be highly engaged and stay for the long term, and it usually results in a much higher ROI for the sender.

Hidden field

Applying a hidden field on your sign-up form is a great way to differentiate automated bot sign-ups from real human subscribers. Because the data field isn't visible, hidden in the HTML code, a bot will enter data where a human wouldn't. Using this method, you can build rules to suppress any sign-up that includes data populated in that hidden field.

reCAPTCHA

reCAPTCHA is a validation method you can use to reduce the chances the subscriber is a bot and not a real person. There are various versions, some of which contain keyword identification or images. Some versions are more effective than others, and what you gain in security and deliverability issue prevention is much higher than any negative impact to conversions.

8.1.3. Legal guidelines

Consult your lawyers to interpret local and national laws concerning email. Remember that email laws widely from amongst different countries and in some cases different local regions within a country.

- Be sure to collect a subscriber's location information so that you're compliant with the subscriber's country laws. Without that detail, you may be limited in how you can market to the subscriber.
- Any relevant laws are generally determined by the location of the recipient, not the sender. So you'll need to know and follow the laws for any country where you might have a subscriber.
- It's often difficult to know with total certainty the country of residence for the subscriber. Data provided by the customer may be out of date, and pixel location data may be inaccurate due to VPN or image warehousing, like with Gmail and Yahoo. When in doubt, it's usually safest to apply the strictest possible laws and guidelines.

8.1.4. Other non-recommended list collection methods

There are many other ways to collect addresses, each with its own opportunities, challenges, and drawbacks. We don't recommend these in general, since use is often restricted via provider acceptable use policies. We'll take a look at a few common examples, so you can learn the dangers to help you limit or avoid the risks:

Buy or rent a list

There are a lot of types of email addresses out there. Primary email, work emails, school emails, secondary emails, and inactive emails to name a few. The types of addresses collected and shared out through these methods are rarely primary email accounts, which is where nearly all engagement and purchase activity occurs.

If you're lucky, you get secondary accounts, where people will look for deals and offers when they're ready to shop for something. This usually results in low engagement levels—if any. If you're not lucky, the list will be full of inactive emails, which may now be spam traps. Often, you get a mix of both secondary and inactive emails. In general, the quality of these types of lists will do more harm than good to an email program. This practice is prohibited by the Adobe Campaign Acceptable Use Policy.

List append

These are customers who have chosen to engage with your brand, which is great. But they chose to engage through a method other than email (in-store, social media, etc.). They may not be receptive to getting an unrequested email from you and may also be concerned about how you gained their email address since they didn't provide it. This method has a risk of turning a customer or potential customer who engaged with your brand into a detractor who no longer trusts

your brand and will go to your competition instead. This practice is prohibited by the Adobe Campaign Acceptable Use Policy.

Trade show or other event collection

Collecting addresses at a booth or through another official, clearly branded method can be useful. The risk is that many events like this collect all addresses and distribute them through the event promoter or host. This means the users of these email addresses never specifically requested to receive emails from your brand. These subscribers are likely to complain and mark your mail as spam, and they may not have provided accurate contact information.

Sweepstakes

Sweepstakes provide large numbers of email addresses quickly. But these subscribers want the prize, not your emails. They may not have even paid attention to the name of who would be reaching out to them. These subscribers are likely to complain and mark your mail as spam, and they may be unlikely to ever engage or make a purchase.

8.2. Welcome emails

8.2.1. Developing a welcome strategy

Your welcome emails are the biggest foundational factor in driving a successful email program. On average, subscribers who engage with your welcome emails are more than four times as likely to continue engaging with other emails you send if you send a single welcome email. Plus, they're 12 times more likely to continue engaging if you send a series of three welcome emails.

Regardless of your strategy, subscribers who don't receive a welcome email at all or who don't connect with your welcome message are unlikely to convert into happy subscribers. A well-planned and carefully crafted welcome plan—that includes thinking about the what, when, and who of your messages—leads to a positive first impression and the best path to long term subscriber satisfaction.

8.2.2. Key elements

Here are a few key elements to consider when building your welcome email or emails:

Send your message ASAP

If you're offering a promotion, your new subscriber will likely be waiting on the website to get the email before making their purchase. A delay of even 5–10 minutes here can mean a lost sale. Even if you don't have a promotion, they're currently expressing interest in your brand. So you need to engage with them while their interest is peaked instead of taking a chance at a later time.

Create strong subject lines and preheaders

You need to not only thank them for signing up—you also need to catch their attention and give them a reason to want to open the email. Don't forget to capitalize on the extra room in the preheader to make your case.

Set expectations

Make it clear that your focus is on a positive experience for them. State what they should expect from you and how often to expect it. Providing a way for them to easily manage their experience (i.e., a link to a preference center) is also a good idea. Also consider adding links to prior content so that users can reference the content they are subscribing to.

Let them get a feel for your brand

Every brand has a voice. Let yours be clearly displayed in your welcome email. This helps your new subscriber connect more with the brand and avoids them feeling surprised by a change in style with later emails.

Keep it concise

You have a lot to say and an eager ear in your new subscriber. But your first message should be short, simple, to the point, and not overwhelming.

Send a series of emails

As noted previously, you have a lot to say to an attentive audience. Building a full welcome series (3–5 emails) allows you to keep each of them to the point while still covering all the information you want to share. It also fosters continued interest from the subscriber, which leads to continued positive engagement, boosted reputation, and improved deliverability.

Get personal

If you're doing a series of welcome emails, use one of them to show the personal touch. Use any information you collected at sign-up or from their purchase to showcase how you can make their experience unique and more valuable to them. If you didn't collect any data yet, use this as an opportunity to show what you could do if given the chance. Then, ask them for the information you need to enrich their experience.

9. Content best practices for optimal deliverability

Content is key. You've already read our perspective on relevance, but here are a few additional tips to optimizing your deliverability when it comes to content:

- **Avoid too large of an HTML file.** Stay under 100KB, but try to stay between 60 and 80KB to prevent slow delivery.
- **Use alt tags to your advantage.** Alt tags live within the image code of the HTML and display text if the image isn't visible or loading. Rather than having a simple description like "product shot," you might want to say something more compelling like, "**Buy now and get 30% off**."
- **Avoid too many images.** Most ISPs now block images by default. You want to have a way to capture your audience without the images enabled so they then enable them.

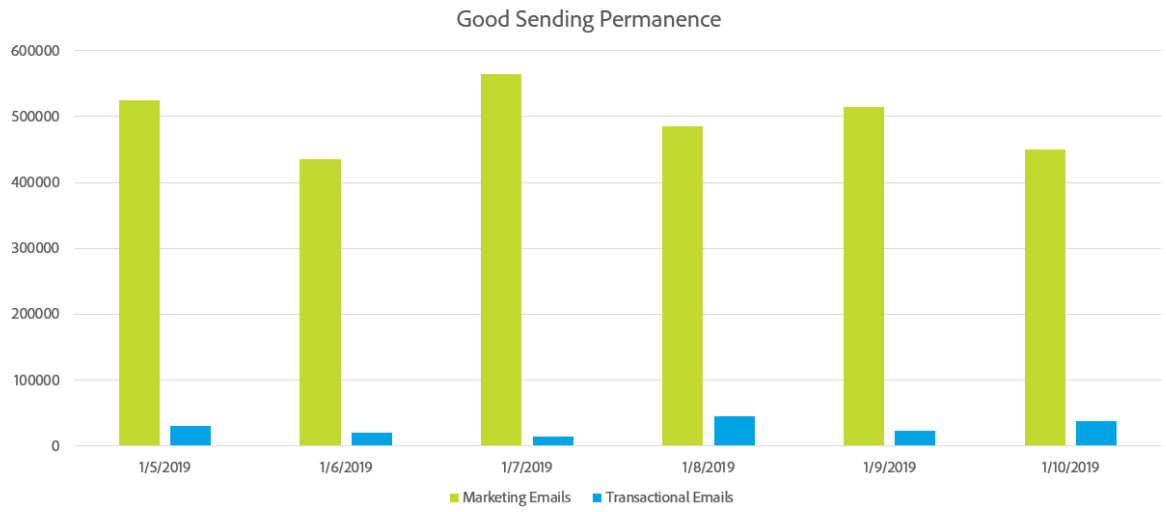
10. Sender permanence

Sending permanence is the process of establishing a consistent sending volume and strategy in order to maintain ISP reputation. Here are some reasons why sender permanence is important:

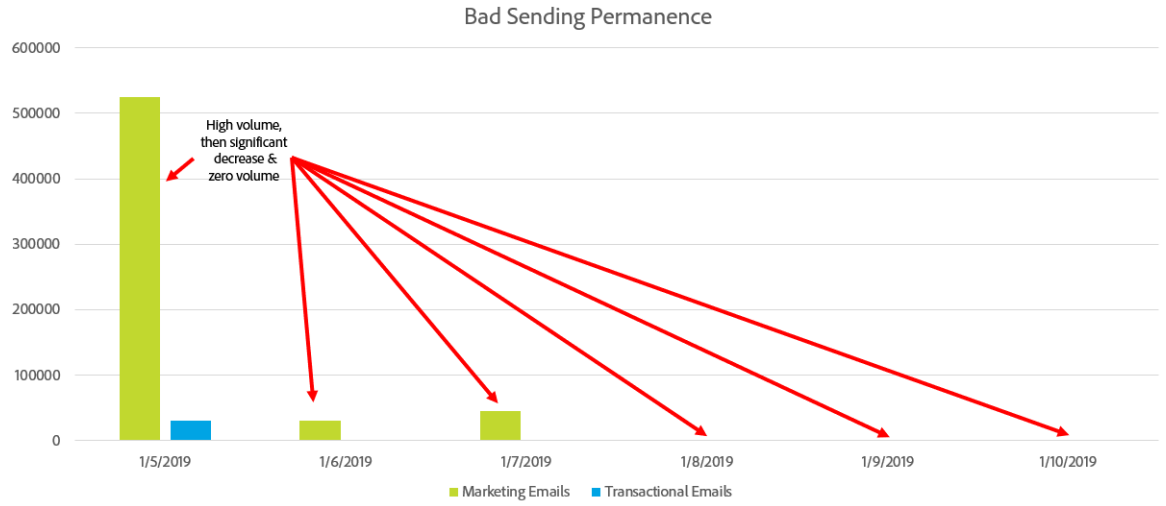
- Spammers will typically "IP address hop," meaning that they'll constantly shift traffic across many IP addresses to avoid reputation issues.
- Consistency is key to prove to ISPs that the sender is reputable and not attempting to bypass any reputation issues that are a result of poor sending practices.
- Maintaining these consistent strategies over a long period of time is required before some ISPs will even consider the sender reputable at all.

Here are some examples:

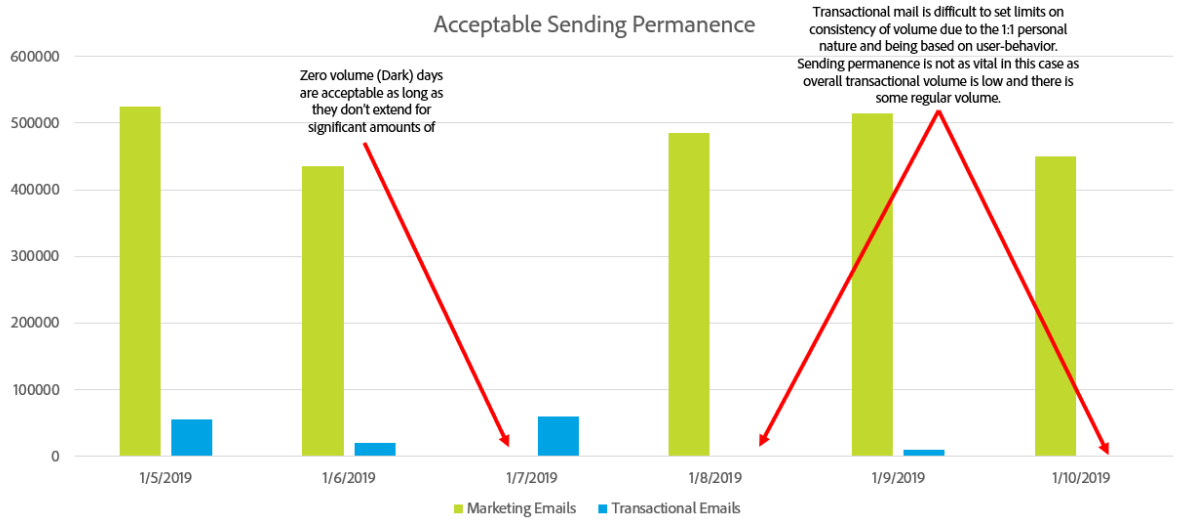
Sender Permanence – Graphical explanation



Sender Permanence – Graphical explanation



Sender Permanence – Graphical explanation



11. Internet service provider specifics

ISPs aren't all the same. They focus on different things when determining what email to allow through to their users' inbox and what email gets filtered to the spam folder or not let through at all. We'll take a quick tour of the important differences between a handful of the ISPs. It's not meant to be a full list of all ISPs or cover all possible differences.

11.1. Gmail

Gmail makes up the largest portion of most senders' email lists. They also tend to treat email a bit differently than everyone else. Here are some highlights:

11.1.1. What data is important?

Gmail is focused on their users' feedback for much of their filtering decisions. While we can't know the secret sauce involved in these decisions, there are common standards that most marketers can monitor. Open and click rates will provide insight into the engagement of your target audience and can be used to drive positive reputation and high inbox placement.

11.1.2. What data is available?

Gmail does provide limited insight into how they view your sending practices through their Gmail Postmaster Tools. This tool allows you a high-level view of your sending IP and domain reputation, authentication results, and complaint issues.

Note: Gmail doesn't display data on all complaints, nor do they facilitate a traditional FBL. Instead, they only provide data in certain circumstances, usually involving both high volumes and very high complaint rates. While keeping complaints to minimum is key to good deliverability, it's

natural for some complaints to filter in. If complaints are regularly clocking at zero, it could point to an issue that requires additional investigation.

11.1.3. Sender reputation

Gmail tracks IP, domain, and even brand reputation. Changing your IP or domain (or both) won't allow you to easily shake a bad reputation. A quick or creative fix may be tempting, but it's much more effective to allocate time and effort to fixing the root of a reputation issue for inbox placement gains.

11.1.4. Insights

Gmail views engaged subscribers differently than most senders traditionally do. A sender may define an active or engaged list as someone who has opened an email within 30, 90, or 180 days (depending on the business model). Gmail, on the other hand, is looking at how often their users interact with your messages.

For instance, if you send 3 emails a week over 90 days, that would be roughly 39 emails. Using the traditional method, if the subscriber opened one of those 39 emails, they're engaged. To Gmail, this means they ignored 38 emails and are *not* engaged. You can get an approximate feel for your own users' *engagement* levels at Gmail by grading them on open count over the last 10 emails. So a subscriber associated with 7 opens of your last 10 emails is more engaged than someone who opened 2 of the 10. Sending email less often to those users who are less engaged will help you improve your sending reputation at Gmail.

Gmail utilizes different tabs for users to distinguish different types of mail. These are "Inbox," "Social," and "Promotional." Even if mail is delivered into the Promotional tab, it's still considered inbox delivery. Users have control to modify their view and tabs.

11.2. Microsoft (Hotmail, Outlook, Windows Live, etc.)

Microsoft is generally the second- or third- largest provider depending on the makeup of your list, and they do handle traffic slightly different from other ISPs.

Here are some highlights:

11.2.1. What data is important?

Microsoft focuses on sender reputation, complaints, user engagement, and their own group of trusted users (also known as Sender Reputation Data or SRD) who they poll for feedback.

11.2.2. What data do they make available?

Microsoft's proprietary sender reporting tool, Smart Network Data Services (SNDS), lets you see metrics around how much mail you are sending and how much mail is accepted, as well as complaints and spam traps. Keep in mind that the data shared is a sample and doesn't reflect exact numbers—but it does best represent how Microsoft views you as a sender. Microsoft doesn't provide information on their trusted user group publicly, but that data is available through the Return Path Certification program for an additional fee.

11.2.3. Sender reputation

Microsoft has been traditionally focused on sending IP in their reputation evaluations and filtering decisions. They're actively working on expanding their sending domain capabilities as well. Both are largely driven by the traditional reputation influencers, like complaints and spam traps. Deliverability can also be heavily influenced by the Return Path Certification program, which does have specific quantitative and qualitative program requirements.

11.2.4. Insights

Microsoft combines all of their receiving domains to establish and track sending reputation. This includes Hotmail, Outlook, MSN, Windows Live, and so on, as well as any corporate Office 365 hosted emails. Microsoft can be especially sensitive to fluctuations in volume, so consider applying specific strategies to ramp up and down from large sends as opposed to allowing for volume-based sudden changes.

Microsoft is also especially strict during the initial days of IP warming, which generally means most mail gets filtered initially. Most ISPs consider senders innocent until proven guilty. Microsoft is the opposite and considers you guilty until you prove yourself innocent.

11.3. Verizon Media Group (Yahoo, AOL, Verizon, etc.)

Verizon Media Group is generally one of the top three domains for most B2C lists. They behave somewhat uniquely, as they'll generally throttle or bulk mail if reputation issues arise.

Here are some highlights:

11.3.1. What data is important?

Verizon Media Group (VMG) has built and maintains their own proprietary spam filters, using a mixture of content and URL filtering and spam complaints. Along with Gmail, they're one of the early adopting ISPs that filter email by domain as well as IP address.

11.3.2. What data do they make available?

VMG has an FBL used to feed complaint information back to senders. They are also exploring adding more data in the future.

11.3.3. Sender reputation

A sender's reputation is made up of a combination of IP address, domain, and from address. Reputation is calculated using the traditional components, including complaints, spam traps, inactive or malformed addresses, and engagement. VMG uses rate limiting (also known as throttling) along with bulk foldering to defend against spam. They complement their internal filtering systems with some Spamhaus black lists, including the PBL, SBL, and XBL to protect their users.

11.3.4. Insights

VMG has regular maintenance periods for old, inactive, email addresses lately. That means it's common to observe a significant surge in invalid address bounces, which may impact your delivered rate for a short period of time. They're also sensitive to high rates of invalid address bounces from a sender, which is indicative of a need to tighten acquisition or engagement policies. Senders can often experience negative impact at around 1 percent invalid addresses.

12. Ongoing monitoring

Here are some ways to help identify a possible issue where you might need expert support:

- There's an observed spike in hard or soft bounces. This could be indicative of a block, blocklisting, or other deliverability issue.
- There's a noticeable decrease in open and click metrics while delivered rates remain high. This is indicative of potential bulk folder placement.
- There's a significant increase in complaints. This can be caused by a poor-quality list source.
- You have any strategic initiatives that might impact deliverability. These include but aren't limited to subscriber acquisition, engagement strategies, seasonal strategies or significant changes to frequency, and campaign type.

13. Putting it in practice

As we've covered in this guide, there are many nuances to deliverability and following best practices. There are four key pillars to success.:

1. Set proper expectations during sign-up and have a good sign-up process that prevents bad addresses.

2. Provide relevant and timely content.

3. Maintain your lists by removing addresses that become bad.

4. Monitor, test, and adjust as you go.

If you're ever unclear or need assistance with an issue, please contact your Adobe deliverability consultant or deliverability expert for help.

14. Sources

Heinz Tschabitscher, "How Many People Use Email Worldwide?," Lifewire, June 24, 2019.

Lori Lewis, "2019: This Is What Happens in an Internet Minute," Merge, March 5, 2019.